BND
Bank of North Dakota

Security Information

A secure online environment is a top priority for Bank of North Dakota (BND). Extensive information security systems and procedures have been implemented to ensure that when you work with BND, your identity and transactions are secure.

BND will never send emails requesting customers to disclose or verify personal information about their accounts. If you receive a suspicious email or phone call, or suspect that fraudulent activity is affecting your accounts, please contact BNDIS@nd.gov.

There are a number of steps you can take to protect yourself from identity theft. A few of them are described for you below.

Passwords and securing your account

If someone you don't know asks for the keys to your home or car, you would likely respond with a "no!" Protect your passwords with the same vigilance.

- Create passwords with a minimum of eight characters and a mix of upper and lowercase letters, numbers and symbols.
- Avoid names of spouses, children and pets as well as birthdates because it is easy for a cybercriminal to figure them out. Instead, use something unique to your life like "IloveApples4" or "3BlueCars#."
- Choose a different password for each online account.
- Write down passwords and store them in a safe place away from your computer or utilize a password management tool.
- Change your password several times a year.

Back it up

Computer malfunctions, cyber theft, viruses, spyware, accidental deletion and natural disasters can cause you to lose important information stored on your computer.

- Make sure your computer has a backup software program and set it to run frequently.
- Use flash drives, an external hard drive or an online backup service to store backup data.
- Keep your backup device somewhere safe and close so you can retrieve it easily.

Update system codes (Patch management)

It is essential that you keep your system up-to-date by installing new patches as they are released. Patches from trusted vendors (like Microsoft or Apple) often include important security updates that help keep your computer safe. If you don't install updates as soon as they come out, you are vulnerable to attacks that can lead to costly downtime.

Establish relationships with application vendors to ensure you receive patches on a regular basis. This can include a subscription to the vendor's security announcement list or phone calls with the vendor. Public websites and mailing lists should be monitored as well.

Click here for more information on patch management.

Safe Internet surfing

Checking out a new website may cause issues like annoying popups or viruses and malware taking over your computer. Follow these tips to prevent problems:

- Visit trusted sites with a valid security certificate.
- Avoid pornography sites. They are hotspots for dangerous malware.
- Be careful when asked to complete personal information like credit card account numbers.
- Clear your browser cache regularly.
- Be careful when using download managers. While it makes downloading easier and quicker, it opens you up to another potential source of malware.

If you think you are a victim of a cybercrime:

- The local law enforcement office should be your first contact. Even if the crime was initiated from another state or country, start with your local officials.
- You may also want to report the incident to one or both of these national programs:
    - The Internet Crime Complaint Center (IC3) thoroughly reviews and evaluates complaints before referring them to the appropriate federal, state, local or international law enforcement or regulatory agency. File your complaint online.
    - FTC Complaint Assistant is operated by the Federal Trade Commission. It is a secure online database used by civil and criminal law enforcement authorities worldwide to detect patterns of cybercrimes. File your complaint online.